

APPROXIMATE (ABELIAN) GROUPS

TOM SANDERS

ABSTRACT. Our aim is to discuss the structure of subsets of Abelian groups which behave ‘a bit like’ cosets (of subgroups). One version of ‘a bit like’ can be arrived at by relaxing the usual characterisation of cosets: a subset S of an Abelian group is a coset if for every three elements $x, y, z \in S$ we have $x + y - z \in S$. What happens if this is not true 100% of the time but is true, say, 1% of the time? It turns out that this is a situation which comes up quite a lot, and one possible answer is called Freiman’s theorem. We shall discuss it and some recent related quantitative advances.

1. INTRODUCTION

The aim of this article is to cover some of the recent developments in the theory of approximate Abelian groups. Our starting point is a common characterisation of cosets of subgroups: suppose that G is an Abelian group and $A \subset G$ is a coset of a subgroup of G – we call this a coset *in* G . A simple characterisation of A being a coset in G is that

$$(i) \ A \neq \emptyset; \text{ and } (ii) \ x, y, z \in A \Rightarrow x + y - z \in A.$$

The theory of approximate groups is concerned with relaxing these conditions. Relaxing the first does not deliver particularly exciting results; relaxing the second, however, turns out to be very fruitful.

Our relaxations will be statistical in nature, and so we shall think of G as being discrete and endowed with Haar counting measure. It follows that we shall be interested in finite sets A . We write

$$E(A) := \sum_{x, y, z \in G} 1_A(x) 1_A(y) 1_A(z) 1_A(x + y - z),$$

a quantity which is called the *additive energy* of A . We see that A is a coset if and only if (it is non-empty) and $E(A) = |A|^3$. Our first question is what happens if condition (ii) is true only a proportion $1 - \delta$ of the time. In particular, what do sets A look like for which

$$(1.1) \quad E(A) \geq (1 - \delta)|A|^3,$$

where δ is to be thought of as a small constant, say $\delta \leq 1/10$, and $|A|$ is to be thought of as tending to infinity.

It is instructive to begin with some examples. The natural way to create sets with this property is based around cosets in G . Indeed, suppose that H is a coset in G and A is any set satisfying

$$|A \cap H| \geq (1 - \epsilon)|A| \text{ and } |A \cap H| \geq (1 - \eta)|H|.$$

In words this says that $1 - \epsilon$ of A is contained in a coset H , and $1 - \eta$ of H is in the intersection of A and H . Then, after a short calculation, we find that

$$E(A) \geq (1 - O(\epsilon + \eta))|A|^3.$$

It turns out that sets constructed in the above way are essentially the *only* sets with large additive energy in the sense of (1.1). The following result is classical and has been considered in far more generality than the statement here suggests. A proof can be read out of Fournier [Fou77], but it seems likely that it was known before then.

Proposition 1.1. *Suppose that G is an Abelian group and $A \subset G$ is finite with $E(A) \geq (1 - \delta)|A|^3$. Then there is some coset H in G such that*

$$|A \cap H| \geq (1 - O(\delta^{1/2}))|A| \text{ and } |A \cap H| \geq (1 - O(\delta^{1/2}))|H|.$$

The main strength of this result is that it is a rough equivalence: every set satisfying the conclusion also satisfies the hypothesis with δ replaced by $O(\delta^{1/2})$ so that up to powers the hypothesis and conclusion are equivalent.

The main weakness of the result is that there may be very few sets satisfying the hypothesis. For example, suppose that $G = \mathbb{Z}/p\mathbb{Z}$ where p is a prime. Then G has no non-trivial subgroups, so if A is of ‘intermediate’ size then a short argument from Proposition 1.1 tells us we must have $E(A) \leq (1 - \Omega(1))|A|^3$; equivalently, no set of ‘intermediate’ size satisfies the hypothesis.

This weakness highlighted in the above discussion can be rectified by a further relaxation of condition (ii), and this is the main concern of the paper. We ask what happens if condition (ii) is true only a proportion δ of the time. In particular, what do sets A look like for which

$$(1.2) \quad E(A) \geq \delta|A|^3,$$

where this time δ is to be thought of as tending to 0 (if at all) much more slowly than $|A|$ tends to infinity.

Once again we start by trying to construct examples of such sets. As before we can use cosets to generate a large class of sets with large additive energy (in the sense of (1.2) this time), but what is more interesting is that a genuinely new sort of structure emerges, that of arithmetic progressions.

If P is an arithmetic progression a short calculation shows that $E(P) \sim \frac{2}{3}|P|^3$, but it turns out that this is just one example from a much wider class.

Definition 1.2 (Convex coset progressions). A *convex progression* in G is a set of the form $\phi(Q \cap \mathbb{Z}^d)$ where Q is a symmetric convex body about the origin in \mathbb{R}^d , and $\phi : \mathbb{Z}^d \rightarrow G$ is a homomorphism. A *convex coset progression* in G is then a set $H + P$ where P is a convex progression and H is a coset in G . In both cases we say that the progression is *d-dimensional*.

It is worth making two small remarks here. First, dimension is monotonic so that if a convex coset progression M is d -dimensional then it is also d' -dimensional for all $d' \geq d$; secondly, in this article we are only interested in dimension up to a constant multiple.

Crucially convex coset progressions inherit growth properties from the convex body used in their definition. It is not hard to show that if M is a convex coset progression then

$$|M + M| \leq \exp(O(d))|M|.$$

We now return to constructing sets with large additive energy. Suppose that M is a d -dimensional convex coset progression and A is any set satisfying

$$|A \cap M| \geq \eta|A| \text{ and } |A \cap M| \geq \epsilon|M|.$$

Then a short calculation using the fact that $|M + M| \leq \exp(O(d))|M|$ tells us that

$$E(A) \geq \epsilon\eta^3 \exp(-O(d))|A|^3.$$

Again it turns out that sets constructed in the above way are essentially the only sets having large additive energy. The following result captures this fact and is a combination of the Balog-Szemerédi Lemma [BS94] and the Green-Ruzsa Theorem [GR07]. It should be remarked that the Green-Ruzsa Theorem is also called Freĭman's theorem for Abelian groups and extends Freĭman's theorem [Fre66] from \mathbb{Z} to general Abelian group.

Theorem 1.3. *Suppose that G is an Abelian group and $A \subset G$ is finite with $E(A) \geq \delta|A|^3$. Then there is a convex coset progression M such that*

$$|A \cap M| \geq \eta(\delta)|A|, |A \cap M| \geq \epsilon(\delta)|M| \text{ and } \dim M \leq d(\delta),$$

for some (increasing) functions η, ϵ and d .

While the result is appealing in its own right, since the breakthrough work of Gowers [Gow98] it has become a central result in additive combinatorics and allied areas as a result of numerous applications. This wealth of applications provides strong empirical evidence for the utility of the theorem, but there are also some rather compelling theoretical reasons why it should be so useful. We turn to some of these now.

- (i) The hypothesis of the theorem is robust under small perturbations. This is particularly useful because while the input is flexible, the output, a convex coset progression, is rather rigid.
- (ii) The hypothesis of the theorem is easily satisfied. From a theoretical perspective this is because convex coset progressions are ubiquitous in contrast to subgroups (in some groups).
- (iii) A convex coset progression supports a lot of structure. While it is not a coset, it behaves enough like a coset that it can support many commonly used analytic arguments, and in particular a sort of approximate harmonic analysis. This means that many results for groups can also be established for convex coset progressions.
- (iv) The result is a rough equivalence: any set satisfying the conclusion of the theorem satisfies the hypothesis with δ replaced by $\epsilon(\delta)\eta(\delta)^3 \exp(-O(d(\delta)))$.

The quality of the rough equivalence serves as a measure of the strength of Theorem 1.3 and conjecturally this equivalence is polynomial. Our interest in this paper is in the quality

of this equivalence – the strength of the bounds on $\eta(\delta)$, $\epsilon(\delta)$ and $d(\delta)$ – the stronger they are the stronger the results in applications. Conjecturally we can take

$$\log \eta(\delta)^{-1}, \log \epsilon(\delta)^{-1}, d(\delta) = O(\log \delta^{-1})$$

in Theorem 1.3. This is called the Polynomial Freĭman-Ruzsa conjecture, and if true means that any set satisfying the output of Theorem 1.3 automatically satisfies the hypothesis with δ replaced by $\delta^{O(1)}$ – the rough equivalence would be rather strong.

Combining Gowers' refinement of the Balog-Szemerédi Lemma [Gow98] with the Green-Ruzsa Theorem [GR07] gives

$$\log \eta(\delta)^{-1}, \log \epsilon(\delta)^{-1}, d(\delta) = O(\delta^{-O(1)}).$$

Green and Ruzsa actually gave an explicit value for the constant implied in the $O(1)$ term and there was some work improving this constant before an important breakthrough by Schoen [Sch11] who showed that it is smaller than any power. Specifically he proved that one may take

$$(1.3) \quad \log \eta(\delta)^{-1}, \log \epsilon(\delta)^{-1}, d(\delta) = O(\exp(O(\sqrt{\log \delta^{-1}}))).$$

Following on from this we were recently able to show in [San10] that

$$(1.4) \quad \log \eta(\delta)^{-1}, \log \epsilon(\delta)^{-1}, d(\delta) = O(\log^{O(1)} \delta^{-1}).$$

The results we have chosen to mention above are far from a complete history of work on Theorem 1.3. Indeed, as a centrepiece of additive combinatorics it has been investigated from many different angles, but we do not have the space to discuss these here. The interested reader may wish to consult the notes [Ruz09] of Ruzsa.

2. DE-COUPLING THE ARGUMENT

The arguments to prove Theorem 1.3 separate naturally into two parts: one more combinatorial, and one more algebraic. The quality of the bounds is almost entirely dependent on the combinatorial part of the argument and that is where most of the recent progress has been made, so we shall now briefly explain how to de-couple the two parts so that we can then focus on the combinatorial one.

The algebraic part of the argument essentially shows that being a convex coset progression is equivalent to satisfying a relative polynomial growth condition. The latter condition is easier to satisfy combinatorially, so that proving Theorem 1.3 comes down to finding a set with relative polynomial growth rather than a convex coset progression.

To be more concrete we start with an observation about convex sets: if Q is a convex set in \mathbb{R}^d then $\mu(nQ) \leq n^d \mu(Q)$ for all $n \geq 1$, and this property is inherited by d -dimensional convex coset progressions. We say that a set X has *relative polynomial growth of order d* if

$$|nX| \leq n^d |X| \text{ for all } n \geq 1,$$

where $nX := X + \dots + X$ and the sum is n -fold¹. It turns out that if M is a d -dimensional coset progression then M has relative polynomial growth of order $O(d)$, and that having

¹In particular $nX := \{x_1 + \dots + x_n : x_1, \dots, x_n \in X\}$.

relative polynomial growth is essentially characteristic for convex coset progressions. To this end we have the following theorem.

Theorem 2.1. *Suppose that G is an Abelian group and $X \subset G$ has relative polynomial growth of order d . Then there is a (centred) convex coset progression M in G such that*

$$X - X \subset M, |M| \leq \exp(O(d \log d))|X| \text{ and } \dim M = O(d \log d).$$

We shall sketch the proof of this Theorem in §8, but it is not the focus of the paper and is more or less a rearrangement of the ideas in Green and Ruzsa [GR07].

By considering the $N \times \cdots \times N$ cube in \mathbb{Z}^d we see that the result is tight up to the logarithmic factors and we think of it as providing an equivalence between d -dimensional convex coset progressions and sets with relative polynomial growth of order d . Indeed, instead of proving Theorem 1.3 we shall prove the following.

Theorem 2.2. *Suppose that G is an Abelian group and $A \subset G$ is such that $E(A) \geq \delta|A|^3$. Then there is a set Y which is a translate of $X - X$ such that*

$$|A \cap Y| \geq \eta'(\delta)|A|, |A \cap Y| \geq \epsilon'(\delta)|Y| \text{ and } |nX| \leq n^{d'(\delta)}|X| \text{ for all } n \geq 1$$

for some (increasing) functions η', ϵ' and d' .

We should like to combine Theorems 2.1 and 2.2 to get Theorem 1.3. We can not do this directly but it turns out that by delving a little into the proofs of each one can combine them to do so, and in particular the ways we establish Theorem 2.2 for given functions η', ϵ' and d' lead to arguments for establishing Theorem 1.3 with $\eta \approx \eta', \epsilon \approx \epsilon'$ and $d \approx d'$.

3. OVERVIEW OF THE COMBINATORIAL OBSTACLES

Our goal now is to prove Theorem 2.2, and in light of the equivalence mentioned in the previous section we shall think of cosets, convex coset progressions and sets with relative polynomial growth as being the same thing for the purpose of constructing examples.

One of the reasons that proving Theorem 2.2 (and hence Theorem 1.3) is hard (and also one reason it is so powerful) is that there are qualitatively three different sorts of structure having large additive energy. We got a sense of roughly what these are earlier but it is helpful now to record them a little more precisely.

- (i) (*Random sets*) Suppose that H is a coset in G and $A \subset H$ is chosen by including each $h \in H$ independently with probability δ . Then (with high probability) $E(A) \approx \delta|A|^3$.
- (ii) (*Independent copies of the same coset*) Suppose H is a coset in G and A is a union of $k \sim \delta^{-1}$ independent cosets in G/H . To be clear this means that $A = \bigcup_{i=1}^k (x_i + H)$ where $\{x_i + H\}_{i=1}^k$ is a set of k elements of H such that

$$n \in \mathbb{Z}^k \text{ and } n_1x_1 + \cdots + n_kx_k \in H \Rightarrow n_ix_i \in H \text{ for all } i \in \{1, \dots, k\}.$$

Then $E(A) \approx \delta|A|^3$.

- (iii) (*Independent copies of different cosets*) Suppose that $k \sim \delta^{-1/2}$ and H_1, \dots, H_k are ‘internally independent cosets’ all of the same size which is to be taken to mean that

$$|H_1 + \dots + H_k| = |H_1| \dots |H_k|,$$

and intuitively means that there are no non-trivial relations between elements in the H_i s. Then $E(A) \approx \delta|A|^3$.

It is a little easier to unify the first two classes of example with each other than the third with either of the first two. This is because in the first two classes there is an obvious choice of coset: H . (In fact the obvious choice is really of subgroup, but this turns out not to be an important distinction here.) On the other hand in the third class any of the cosets (or, rather, corresponding subgroups of) H_1, \dots, H_k are reasonable choices and there is no particular reason to pick one over the other.

A unifying aspect of the first two classes above is that the sets A given have small sumset. In particular, in both classes we have that $|A + A| = \Theta(\delta^{-1}|A|)$ which we think of as saying that A has ‘small doubling’; in the third class $|A + A| = \Omega(|A|^2)$ so that it is almost as large as can be.

The first step in proving Theorem 2.2 is then in converting sets from the third class into the first two, and this is the purpose of the Balog-Szemerédi-Gowers Lemma. Qualitatively this was proved by Balog and Szemerédi in [BS94], but it was a very important step when Gowers established polynomial bounds in [Gow98].

Theorem 3.1 (Balog-Szemerédi-Gowers Lemma). *Suppose that $A \subset G$ has $E(A) \geq \delta|A|^3$. Then there is a set $A' \subset A$ such that*

$$|A'| \geq \delta^{O(1)}|A| \text{ and } |A' + A'| \leq \delta^{-O(1)}|A'|.$$

This result has been studied extensively elsewhere and will not be our focus here. The interested reader might like to consult the book [TV06] of Tao and Vu. It is worth saying that the proof is elementary, albeit rather clever, and is set around the idea of examining $A \cap (x + A)$ for suitable randomly chosen x . In the third class of examples considered above this has the effect of selecting one of the cosets (at random).

From now on we shall be interested in the case of so-called ‘small doubling’ mentioned earlier meaning the case when $|A + A| \leq K|A|$, and shall prove the following.

Theorem 3.2. *Suppose that G is an Abelian group and $A \subset G$ is such that $|A + A| \leq K|A|$. Then there is a set Y which is a translate of $X - X$ such that*

$$|A \cap Y| \geq \eta''(K)|A|, |A \cap Y| \geq \epsilon''(K)|Y| \text{ and } |nX| \leq n^{d''(K)}|X| \text{ for all } n \geq 1$$

for some (decreasing) functions η'', ϵ'' and d'' .

This yields Theorem 2.2 on combination with the Balog-Szemerédi-Gowers Lemma with

$$\eta'(\delta) = \delta^{O(1)}\eta''(\delta^{-O(1)}), \epsilon'(\delta) = \delta^{O(1)}\epsilon''(\delta^{-O(1)}) \text{ and } d'(\delta) = d''(\delta^{-O(1)}).$$

In actual fact for the best bounds one also goes into the details of the proof of the Balog-Szemerédi-Gowers Lemma, but for this overview that improvement will not concern us.

The focus of the paper now is on proving Theorem 3.2 and we split into three sections. In §5 we establish Theorem 2.2 with bounds corresponding roughly to the original work of Green and Ruzsa; in §6 we develop Schoen's improvement of this; and, finally, in §7 we develop the improvement leading to the bounds in (1.4).

4. SUMSET ESTIMATES AND POLYNOMIAL GROWTH

In this brief section we record a couple of useful results which will help us to establish relative polynomial growth on all scales from a growth condition on just one scale. In particular we have the following result of Chang [Cha02].

Lemma 4.1 (Variant of Chang's covering lemma). *Suppose that G is an Abelian group and $X \subset G$ is symmetric with $|(3k+1)X| < 2^k|X|$ for some k . Then $|nX| \leq n^k|X|$ for all $n \geq 1$.*

To establish the hypothesis of this lemma it will also be useful to have Plünnecke's inequality.

Theorem 4.2 (Plünnecke's inequality). *Suppose that $|A+A| \leq K|A|$. Then $|nA| \leq K^n|A|$ for all $n \geq 1$.*

This result was proved by Plünnecke in [Plü69], and his proof was rediscovered and popularised somewhat later by Ruzsa. Very recently, however, Petridis [Pet11] found a new proof which is very direct and well worth reading.

Before closing this short section it is worth saying that the above two results are part of a rich family of sumset estimates we do not have time to touch on here, but we direct the interested reader towards Tao and Vu [TV06] for more details.

5. THE BASIC ARGUMENT

We now turn our attention to proving Theorem 3.2 with bounds of the quality arrived at by Green and Ruzsa in [GR07]. We are thus considering a set A with $|A+A| \leq K|A|$ and in light of our earlier discussions we can restrict ourselves to sets coming from the first two classes of structure in §3.

Even with the work we have done the two classes of possible structure behave differently: in the first class when A is chosen randomly from H , A will typically have a lot of gaps so that 1_A is not very smooth. One way of smoothing a function is by averaging or convolving and to this end we make a definition.

Given $f, g \in \ell^1(G)$ we define the *convolution* of f and g to be the function

$$f * g(x) = \sum_{y+z=x} f(y)g(z) \text{ for all } x \in G.$$

To relate this to sets we define some level sets called symmetry sets. Given a set A the *symmetry set at threshold η* is defined to be the set

$$\text{Sym}_\eta(A) := \{x \in G : 1_A * 1_{-A}(x) \geq \eta|A|\}.$$

Note that $1_A * 1_{-A}(x) \leq |A|$ so that $\text{Sym}_\eta(A)$ is the set of points where $1_A * 1_{-A}$ is a proportion η of its maximum.

Heuristically we expect $1_A * 1_A$ to be pretty smooth – on a qualitative level 1_A is an element of L^2 and the convolution of two L^2 functions is continuous. Concretely then we expect to have a quantitative version of the notion of uniform continuity, meaning there should be a (large) set X such that on translation by elements of X , the convolution does not vary very much. To formulate this precisely we define translation: given $f \in \ell^2(G)$ we write

$$\tau_x(f)(y) = f(y + x) \text{ for all } x, y \in G.$$

It will also be helpful to write μ_A for the function $1_A/|A|$ so that $f * \mu_A(x)$ is the average value of f over the set $x - A$. The heuristic above can be made precise in a number of ways but one very powerful approach is due to Croot and Sisask [CS10] who proved the following lemma.

Lemma 5.1 (Croot-Sisask Lemma). *Suppose that G is an Abelian group, $f \in \ell^2(G)$ and $|A + A| \leq K|A|$. Then there is a set X with $|X| \geq (2K)^{-O(\epsilon^{-2})}|A|$ such that*

$$\|\tau_x(f * \mu_A) - f * \mu_A\|_{\ell^2(G)} \leq \epsilon \|f\|_{\ell^2(G)} \text{ for all } x \in X.$$

Sketch proof. The basic idea is to start with the equality

$$f * \mu_A = \mathbb{E}_{a \in A} \tau_{-a}(f).$$

Given this we can randomly sample from A , say k times, and get a good approximation to $f * \mu_A$:

$$f * \mu_A \approx \frac{1}{k} \sum_{i=1}^k \tau_{-z_i}(f)$$

for z_1, \dots, z_k chosen uniformly at random from A . Here ‘ \approx ’ means approximately equal in ℓ^2 -norm, and the larger the value of k , the better the approximation.

We now examine the set L of vectors $(z_i)_{i=1}^k$ such that the approximation is good. By averaging we prove that $L - L$ has a large intersection, call it X , with the diagonal set $\{(a, \dots, a) : a \in A\}$. On the other hand, if $x \in X$ then it follows that there is some $z \in L$ such that

$$f * \mu_A \approx \frac{1}{k} \sum_{i=1}^k \tau_{-z_i-x}(f) \text{ and } f * \mu_A \approx \frac{1}{k} \sum_{i=1}^k \tau_{-z_i}(f)$$

and hence

$$\tau_x(f * \mu_A) \approx f * \mu_A \text{ for all } x \in X.$$

Working through the details of this sketch gives the proof. \square

Given the above result we shall now prove the following which is the version of Theorem 3.2 corresponding to the bounds of Green and Ruzsa although the argument is somewhat different.

Theorem 5.2. *Suppose that G is an Abelian group and $A \subset G$ is such that $|A + A| \leq K|A|$. Then there is a set Y which is a translate of $X - X$ such that*

$$|A \cap Y| \geq \exp(-K^{1+o(1)})|A|, \quad |A \cap Y| = \Omega(|Y|/K)$$

and

$$|nX| \leq n^{K^{1+o(1)}}|X| \text{ for all } n \geq 1.$$

Sketch proof. We let k be a natural number to be optimised later and apply the Croot-Sisask lemma with $\epsilon = 1/2k\sqrt{K}$ to get a set X with $|X| \geq |A|/(2K)^{O(k^2K)}$ such that

$$\|\tau_x(1_A * 1_A) - 1_A * 1_A\|_{\ell^2(G)}^2 \leq |A|^3/4K \text{ for all } x \in kX$$

by the triangle inequality. Now, by Cauchy-Schwarz we have $\|1_A * 1_A\|_{\ell^2(G)}^2 \geq |A|^3/K$ which by the triangle inequality and the output of the Croot-Sisask lemma tells us two things:

$$kX \subset 2A - 2A \text{ and } \|1_A * 1_A * \mu_{X-X}\|_{\ell^2(G)}^2 \geq |A|^3/4K.$$

The second of these gives us the translate Y of $X - X$ such that $|A \cap Y| = \Omega(|Y|/K)$ via an averaging argument; the first let us control the degree of polynomial growth of X .

Since $kX \subset 2A - 2A$ we have by Plünnecke's inequality that

$$|klX| \leq K^{4l}|A| \leq K^{4l}(2K)^{O(k^2K)}|X|.$$

Putting $3r + 1 = kl$ and $l = k^2K$ we get that

$$|(3r + 1)X| \leq K^{O(r^{2/3}K^{1/3})}|X|;$$

it follows that we can take $r = O(K \log^3 K)$ such that $|(3r + 1)X| < 2^r|X|$. Chang's covering lemma then tell us that X has the right order of relative polynomial growth.

Finally from the definition of r and l in terms of k we get that $k = O(\log K)$ from which the bound in the size of $|A \cap Y|/|A|$ follows. \square

6. SCHOEN'S REFINEMENT

Schoen in [Sch11] made a major breakthrough when he proved the bounds mentioned in (1.3). If we study the argument above the weakness was that we had to take $\epsilon \approx 1/\sqrt{K}$ in our application of the Croot-Sisask lemma, and since the resultant set X has size exponentially dependent on ϵ^{-2} this lead to exponential losses in K .

To some extent these losses are necessary as can be seen by considering the examples in class (i) of §3. In this class A is chosen randomly with probability $1/K$ from a coset H , so that (with high probability)

$$1_A * 1_A(x) \approx |A|/K \text{ for all } x \in A - A.$$

On the other hand $A + A$ is very structured – it is the whole coset H . Similarly, in class (ii) of §3, $A + A$ is again very structured.

It follows that in either of the above cases $1_{A+A} * 1_{A+A}$ takes rather large values; certainly much larger than those of $1_A * 1_A$ in the case when A is chosen randomly. If we can guarantee that some convolution takes a lot of values much larger than its average value then the arguments at the end of the last section can be applied much more effectively.

This is roughly speaking Schoen's idea and the following is one of the key ingredients from [Sch11].

Proposition 6.1. *Suppose that G is an Abelian group, A is a finite subset of G with $|A + A| \leq K|A|$, and $\epsilon \in (0, 1]$ is a parameter. Then there is a non-empty set $A' \subset A$ such that*

$$|\text{Sym}_{K^{-\eta}}(A' + A)| \geq \exp(-\exp(O(\eta^{-1})) \log K)|A|.$$

The proof of this is iterative and based around an important observation which seems to have been first made by Katz and Koester in [KK10].

Suppose that $A'' \subset G$ is such that $|A + A''| \leq M|A|$ and $|A'' + A''| \leq L|A''|$. Then we have

$$1_{A+A''} * 1_{-(A+A'')}(x) = |(A + A'') \cap (x + A + A'')| \geq |A + (A'' \cap (x + A''))|.$$

Writing S for the set of x such that $A'' \cap (x + A'')$ is large, that is

$$S := \{x \in G : 1_{A''} * 1_{A''}(x) \geq |A''|/2L\},$$

we have two possibilities:

- (i) either $1_{A+A''} * 1_{-(A+A'')}(x) \geq R|A + A''|$ for all $x \in S$;
- (ii) or, putting $A''' := A'' \cap (x + A'')$, we have

$$|A''' + A'''| \leq 2L^2|A'''| \text{ and } |A + A'''| \leq (M/R)|A|.$$

Given this we proceed by downward induction on $|A + A''|/|A|$ terminating when we are in the first case and repeating with A'' replaced by A''' , M by M/R and L by $2L^2$ in the second. This yields the proposition.

With the above result we can now prove the following.

Theorem 6.2. *Suppose that G is an Abelian group and $A \subset G$ is such that $|A + A| \leq K|A|$. Then there is a set Y which is a translate of $X - X$ such that*

$$|A \cap Y| \geq \exp(-\exp(O(\sqrt{\log K})))|A|, \quad |A \cap Y| = \Omega(|Y|/K^{O(1)})$$

and

$$|nX| \leq n^{\exp(O(\sqrt{\log K}))}|X| \text{ for all } n \geq 1.$$

Sketch proof. We apply Proposition 6.1 and put $S := \text{Sym}_{K^{-\eta}}(A' + A)$ so that

$$|S| \geq \exp(-\exp(O(\eta^{-1})) \log K)|A|.$$

By definition and the Cauchy-Schwarz inequality we have that

$$\|1_{A+A'} * 1_S\|_{\ell^2(G)} \geq K^{-2\eta}|A + A'| |S|,$$

and (since $S \subset 2A - 2A$) that

$$|S + S| \leq \exp(\exp(O(\eta^{-1})) \log K)|S|.$$

We then proceed as in the proof of Theorem 5.2 but this time apply Croot-Sisask to the function $1_{A+A'}$ and the set S with parameter $\epsilon = 1/2kK^{-\eta}$ and get a set X with

$$|(3r + 1)X| \leq (2K)^{O(r^{2/3}K^{O(\eta)} \exp(O(\eta^{-1})))}|X|.$$

Optimising for η we take $\eta = 1/\sqrt{\log K}$, and then the argument proceeds much as before to give the result. \square

7. THE LÓPEZ-ROSS TRICK AND GENERALISED CROOT-SISASK

The Croot-Sisask lemma has a rather powerful generalisation to ℓ^p -norms.

Lemma 7.1 (Croot-Sisask lemma, ℓ^p -norm version). *Suppose that G is an Abelian group, $f \in \ell^p(G)$ and $|A + A| \leq K|A|$. Then there is a set X with $|X| \geq (2K)^{-O(\epsilon^{-2}p)}|A|$ such that*

$$\|\tau_x(f * \mu_A) - f * \mu_A\|_{\ell^p(G)} \leq \epsilon \|f\|_{\ell^p(G)} \text{ for all } x \in X.$$

This result is also from [CS10] and the proof of the ℓ^2 version except that Khintchine's inequality has to be replaced by the Marcinkiewicz-Zygmund inequality.

The reason that this result is so much more powerful than the ℓ^2 version of the Croot-Sisask lemma is in the bounds. In particular the p dependence is exponential in p , rather than doubly exponential which is what all previous arguments had given. To understand why it is useful here we now sketch the proof of the following.

Theorem 7.2. *Suppose that G is an Abelian group and $A \subset G$ is such that $|A + A| \leq K|A|$. Then there is a set Y which is a translate of $X - X$ such that*

$$|A \cap Y| \geq \exp(-\log^{O(1)} K)|A|, \quad |A \cap Y| = \Omega(|Y|/K^{O(1)})$$

and

$$|nX| \leq n^{\log^{O(1)} K}|X| \text{ for all } n \geq 1.$$

Sketch proof. Rather than examining the ℓ^2 -norm of the convolution of two functions we use an observation of López and Ross from [LR75]:

$$\langle 1_{A+A}, 1_A * 1_A \rangle = |A|^2.$$

On the other hand if we know that

$$\|\tau_x(1_{A+A} * 1_A) - 1_{A+A} * 1_A\|_{\ell^p(G)} \leq \epsilon \|1_{A+A}\|_{\ell^p(G)},$$

then we conclude that

$$\langle \tau_x(1_{A+A}), 1_A * 1_A \rangle \geq |A|^2 - \epsilon \|1_{A+A}\|_{\ell^p(G)} |A| = |A|^2(1 - \epsilon K^{1/p}).$$

We conclude that we can take $p \sim \log K$ and $\epsilon = \Omega(1)$ such that

$$\langle \tau_x(1_{A+A}), 1_A * 1_A \rangle \geq |A|^2/2.$$

But this means by the Croot-Sisask lemma that there is a set X of size at least $|A|K^{-O(k^2)}$ such that

$$\langle \tau_x(1_{A+A}), 1_A * 1_A \rangle \geq |A|^2/2 \text{ for all } x \in kX.$$

This can then be plugged back into a similar argument to the ones we had before to get Theorem 7.2.

The advantage here is that the set X we have found is a lot bigger than those we had previously found as a result of the good bounds in the Croot-Sisask lemma. \square

8. POLYNOMIAL GROWTH AND CONVEX PROGRESSIONS

In this section we shall sketch a proof of Theorem 2.1 which we restate now as a reminder.

Theorem 8.1 (Theorem 2.1). *Suppose that G is an Abelian group and $X \subset G$ is such that $|nX| \leq n^d |X|$ for all $n \geq 1$. Then there is a (centred) convex coset progression M in G such that*

$$X - X \subset M, |M| \leq \exp(O(d \log d)) |X| \text{ and } \dim M = O(d \log d).$$

As indicated this is largely a rearrangement of the ideas of Green and Ruzsa in [GR07], which are themselves developed from the hugely influential paper [Ruz94] of Ruzsa.

One of the key tools is the Fourier transform which in this case we define regarding G as a discrete group. We write \widehat{G} for the compact Abelian group of characters on G and given $f \in \ell^1(G)$ the *Fourier transform* of f is defined to be the function

$$\widehat{f} : \widehat{G} \rightarrow \mathbb{C}; \gamma \mapsto \sum_{x \in G} f(x) \overline{\gamma(x)}.$$

There is a useful notion of approximate annihilator on G called Bohr sets. Given $\Gamma \subset \widehat{G}$ a compact set and $\delta \in (0, 2]$ we write

$$\text{Bohr}(\Gamma, \delta) := \{x \in G : |\gamma(x) - 1| \leq \delta \text{ for all } \gamma \in \Gamma\}.$$

Bohr sets interact particularly well with the large spectrum of a set. Given $A \subset G$ we write

$$\text{LSpec}(A, \epsilon) := \{\gamma \in \widehat{G} : \|1 - \gamma\|_{L^2(\mu_A * \mu_{-A})} \leq \epsilon\}.$$

The basic idea is to show that if X has polynomial growth then $X - X$ is contained in the Bohr set of the large spectrum of (a dilate of) X . We then show that this Bohr set is not too large, and finally that it is actually a low dimensional convex coset progression.

The following proposition deals with the first objective above; it is only slightly more general than [TV06, Proposition 4.39].

Proposition 8.2. *Suppose that $X \subset G$, l is a positive integer such that $|lX| \leq K|(l-1)X|$ and $\epsilon \in (0, 1]$ is a parameter. Then*

$$X - X \subset \text{Bohr}(\text{LSpec}(lX, \epsilon), 2\epsilon\sqrt{2K}).$$

The proof is fairly straightforward after unpacking the definitions.

The second objective above – that the Bohr set not be too large – is proved using an idea of Schoen [Sch03] introduced to Freiman-type problems by Green and Ruzsa in [GR07].

Proposition 8.3. *Suppose that $X \subset G$ has $|nX| \leq n^d |X|$ for all $n \geq 1$, and $\epsilon \in (0, 1/2]$ is a parameter. Then we have the estimate*

$$|\text{Bohr}(\text{LSpec}(X, \epsilon), 1/2\pi)| \leq \exp(O(d \log \epsilon^{-1} d)) |X|.$$

The proof of this is via the Fourier transform which shows that the large spectrum of the specified Bohr set must support a lot of the ℓ^2 -mass of 1_X .

To deal with similar concerns to those of our the final objective Ruzsa introduced the geometry of number to Freiman-type theorems in [Ruz94]. There is a great deal to say

about this, and we direct the reader to [TV06, Chapter 3.5] for a much more comprehensive discussion. For our purposes we have the following proposition.

Proposition 8.4. *Suppose that G is an Abelian group, $d \in \mathbb{N}$ and B is a Bohr set such that*

$$|\text{Bohr}(\Gamma, (3d+1)\delta)| < 2^d |\text{Bohr}(\Gamma, \delta)| \text{ for some } \delta < 1/4(3d+1).$$

Then $\text{Bohr}(\Gamma, \delta)$ is a d -dimensional convex coset progression.

The proof of this involves the covering lemma of Chang mentioned earlier and a very important embedding defined by Ruzsa

$$R_\Gamma : G \rightarrow C(\Gamma, \mathbb{R})$$

$$x \mapsto R_\Gamma(x) : \Gamma \rightarrow \mathbb{R}; \gamma \mapsto \frac{1}{2\pi} \arg(\gamma(x)),$$

where the argument is taken to lie in $(-\pi, \pi]$. The map R_Γ acts as something called a Freiman morphism² which lets us embed Bohr sets into a lattice.

With those three ingredients it is possible to stitch together a proof of Theorem 2.1 and the section is complete.

REFERENCES

- [BS94] A. Balog and E. Szemerédi. A statistical theorem of set addition. *Combinatorica*, 14(3):263–268, 1994.
- [Cha02] M.-C. Chang. A polynomial bound in Freiman’s theorem. *Duke Math. J.*, 113(3):399–419, 2002.
- [CS10] E. S. Croot and O. Sisask. A probabilistic technique for finding almost-periods of convolutions. *Geom. Funct. Anal.*, 20(6):1367–1396, 2010.
- [Fou77] J. J. F. Fournier. Sharpness in Young’s inequality for convolution. *Pacific J. Math.*, 72(2):383–397, 1977.
- [Fre66] G. A. Freiman. *Nachala strukturnoi teorii slozheniya mnozhestv*. Kazan. Gosudarstv. Ped. Inst, 1966.
- [Gow98] W. T. Gowers. A new proof of Szemerédi’s theorem for arithmetic progressions of length four. *Geom. Funct. Anal.*, 8(3):529–551, 1998.
- [GR07] B. J. Green and I. Z. Ruzsa. Freiman’s theorem in an arbitrary abelian group. *J. Lond. Math. Soc. (2)*, 75(1):163–175, 2007.
- [KK10] N. H. Katz and P. Koester. On additive doubling and energy. *SIAM J. Discrete Math.*, 24(4):1684–1693, 2010.
- [LR75] J. M. López and K. A. Ross. *Sidon sets*. Marcel Dekker Inc., New York, 1975. Lecture Notes in Pure and Applied Mathematics, Vol. 13.
- [Pet11] G. Petridis. New proofs of Plünnecke-type estimates for product sets in groups. 2011, arXiv:1101.3507.
- [Plü69] H. Plünnecke. *Eigenschaften und Abschätzungen von Wirkungsfunktionen*. BMwF-GMD-22. Gesellschaft für Mathematik und Datenverarbeitung, Bonn, 1969.
- [Ruz94] I. Z. Ruzsa. Generalized arithmetical progressions and sumsets. *Acta Math. Hungar.*, 65(4):379–388, 1994.
- [Ruz09] I. Z. Ruzsa. Sumsets and structure. In *Combinatorial number theory and additive group theory*, Adv. Courses Math. CRM Barcelona, pages 87–210. Birkhäuser Verlag, Basel, 2009.
- [San10] T. Sanders. On the Bogolyubov-Ruzsa lemma. *Anal. PDE*, to appear, 2010, arXiv:1011.0107.

²We direct the unfamiliar reader to [TV06, Chapter 5.3].

- [Sch03] T. Schoen. Multiple set addition in \mathbb{Z}_p . *Integers*, 3:A17, 6 pp. (electronic), 2003.
- [Sch11] T. Schoen. Near optimal bounds in Freĭman’s theorem. *Duke Math. J.*, 158:1–12, 2011.
- [TV06] T. C. Tao and H. V. Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

MATHEMATICAL INSTITUTE, UNIVERSITY OF OXFORD, 24-29 ST. GILES’, OXFORD OX1 3LB,
ENGLAND

E-mail address: tom.sanders@maths.ox.ac.uk